ULTIMATE BACKDOORS - Encryption Compromised Since 2003 or so - Electronic Spying Everywhere With Just About All Devices

I have in the past stated that the always on cell connection in Intel processors made it's debut with Sandy Bridge. BUT, Yesterday I sat down to an ancient computer here in Mexico, that said Windows Vista on it, and Equipped with Intel Corevpro Technology, with the Core2 logo on it. I think it was a Compaq. SO, now we know for sure that the Centrino technology, which was rolled into Core2 and every Intel processor since including the Pentiums and Celerons, have that cell connection on the processor die. With an always on cell connection and Corevpro, you can't encrypt anything on your computer because Corevpro snags all encryption keys and holds them in a separate processor that runs parallel with the main processor and that second processor has as a feature an always on cell connection. It's the ultimate back door.
Centrino was designed exclusively in Israel. They put a permanent back door into every processor they develop, there for their exploit. We have not had any data security with Intel processors since 2003 or so.
The problem is a lot older and a lot worse than I thought. So I will apologize for not warning people how bad it really was, but won't cry with that apology because WHO ELSE OUT THERE WILL SAY IT AT ALL?

I have in the past stated that the always on cell connection in Intel processors made it's debut with Sandy Bridge. BUT, Yesterday I sat down to an ancient computer here in Mexico, that said Windows Vista on it, and Equipped with Intel Corevpro Technology, with the Core2 logo on it. I think it was a Compaq. SO, now we know for sure that the Centrino technology, which was rolled into Core2 and every Intel processor since including the Pentiums and Celerons, have that cell connection on the processor die. With an always on cell connection and Corevpro, you can't encrypt anything on your computer because Corevpro snags all encryption keys and holds them in a separate processor that runs parallel with the main processor and that second processor has as a feature an always on cell connection. It's the ultimate back door.
Centrino was designed exclusively in Israel. They put a permanent back door into every processor they develop, there for their exploit. We have not had any data security with Intel processors since 2003 or so.
The problem is a lot older and a lot worse than I thought. So I will apologize for not warning people how bad it really was, but won't cry with that apology because WHO ELSE OUT THERE WILL SAY IT AT ALL?

Once they got their toe dip with Centrino and Core2, they briefly announced that all I series processors, starting with Sandy Bridge, would have an always on 3g connection connected to the cell network at all times, right from the core of the CPU. This was initially toe dipped as a way to "kill the machine to protect your data if it ever got stolen" as part of a new feature called "anti theft 3.0" but people then said, WELL, that won't kill the hard drive, so the Sandy Bridge processors were released with this feature un

announced after release and the buyers did not get the back door keys needed to kill their machines if they ever got stolen.Yet the back door remained in place for the NSA to rape and pillage with. This has been expunged from the web, but it was a huge topic here.
NOT TO WORRY THOUGH, they made a hugely public announcement with CoreVpro, which proudly and unabashedly announces that ALL corevpro processors have a separate processor the user can never access which does ALL OF THE ABOVE, including snag your encryption keys, have an always open 3g connection that an admin can update all computers in a network with, without them even appearing to turn on including software installs, file transfers and deletes, THE WHOLE 9 YARDS. GOD, the NSA LOVES THAT ONE!. You can't secure a Corevpro machine from ANYTHING other than Aunt Edna.

New Intel based PC's PERMANENTLY hackable
So you think no one can access your data because your computer is turned off. Heck it's more than turned off, you even took the main hard drive out, and only the backup disk is inside. There is no operating system installed at all. So you KNOW you are safe. Frank from across the street is an alternative operating systems hobbyist, and he has tons of computers. He has Free BSD on a couple, his own compilation of Linux on another, a Mac for the wife, and even has Solaris on yet another. Frank knows systems security, so he cannot be hacked . . . . . or so he thinks.
The government does not like Frank much, because they LOVE to look at everything. Privacy is a crime don't you know, and it looks like Frank's luck with privacy is about to run out because his latest and greatest machine was a Corevpro equipped I7.
The new Intel Core vPro processors contain a new remote access feature which allows 100 percent remote acess to a PC 100 percent of the time, even if the computer is TURNED OFF. Core vPro processors contain a second physical processor embedded within the main processor which has it's own operating system embedded on the chip itself. As long as the power supply is available and and in working condition, it can be woken up by the Core vPro processor, which runs on the system's phantom power and is able to quietly turn individual hardware components on and access anything on them. This is being touted as something that makes IT administration easy. It is being advertised as something that will allow IT professionals the ability to remotely troubleshoot a PC no matter what is wrong with it. It allows IT professionals to view the contents of hard drives, check the memory, or hunt for problems on a machine without actually being in front of it. And to that, I call B.S, outside of snooping it's only real world applications would involve accessing a recovery partiton and restoring the computer to out of box state, installing software outside the knowledge of the main operating system, and secretly placing or deleting files.
But the intelligence agencies LOVE THIS. Because Frank is going on vacation soon and they know it. They have listened to all of his calls. They KNOW frank is a terrorist, because they have never been able to access anything Frank has done with a PC, and who would hide their use, other than a criminal? Frank keeps his computers up to date, and THREE of them now have Core vPro processors in them, and when Frank is gone,

they are going to get their chance to access ALL of his files because the main backup hard disk went into the newest machine.
Real world use for Core vPro processors will involve the following:
Accessing any PC ANYWHERE, no matter what operating system is installed, even if it is physically disconnected from the internet. You see, Core vPro processors work in conjunction with Intel's new Anti Theft 3.0, which put 3g connectivity into every Intel CPU after the Sandy Bridge version of the I3/5/7 processors. Users do not get to know about that 3g connection, but it IS there. Frank was not stupid so he unplugged his router. Unfortunately for Frank, that won't work, because anti theft 3.0 always has that 3g connection on also, even if the computer is turned off. Sorry frank, you were good with operating systems, but did not know EVERYTHING about hardware. And now the real reason for your finicky security habits will be known to the NSA - you found a way to route photons to any place in the world without any sort of cable. You revolutionized communications. You were going public when you returned from your vacation, but thanks to your new Core vPro processors, a major communications firm is going to go public with your invention BEFORE you get home, and your research will be deleted and replaced with "criminal activity" so you will be arrested when you get back and unable to speak about the theft of your invention. Fascism is GREAT.
If a system has the ram chips pulled, a Core vPro processor will read the hard disk anyway because it has all the ram it needs embedded in the vPro core.
If you encrypted your hard drive, a Core vPro processor will read it anyway, because it snagged your encryption key
If your system has been taken apart, and has no video card, ram, floppy, or hard drive, your Core vPro processor nailed you, because you left a flash drive plugged in. Or a CD in the CD drive. And what about that web cam?
The bottom line? The Core vPro processor is the end of any pretend privacy. If you think encryption, Norton, or anything else is going to ensure your privacy, including never hooking up to the web AT ALL, think again. There is now more than just a ghost in the machine.
The Zionist, Globalist, Banker scamming war mongering cabal has a history of using the marketing of security as a means to remove ALL security and nail you. If you believe Intel's cheerful hype about these processors making things more secure than ever, think again, because any processor which allows a machine to be accessed even when it's turned off equates to an information tyrant's dream come true Please engage your brain while watching this, the security pitch is unadulterated B.S. These processors in fact represent an ABSOLUTE BREACH of security no matter HOW they are marketed. From the techinical viewpoint of someone who worked for an intelligence agency, I call B.S. on Intel, avoid these processors like the plague!

Got AMD? What about your smart meter?
Many people are interested in the issue of smart meters, and for good reason. Not only does a smart meter have a full time connection to the outside world via the cell phone network, but it also has direct access to the wiring in your house. Is this a cause for concern? I'd say definitely, and this article will outline the reasons why, and show you

the security holes this obvious snooping device has introduced into your home or business.

It has been publicly stated that your smart meter has a one watt wifi transmitter and receiver in it (which is far beyond legal power for little people), as well as a full time 3g or better connection to the cell network which is always on. It is fully admitted that smart meters can communicate with appliances designed to do so, and that eventually all appliances will be able to communicate with it and receive instructions from the meter to modify their functioning on demand from a centralized control center. Seemingly, to assuage fears, it is being stated that the smart meter only communicates with appliances in a minimal way, and I call B.S. on that. I call B.S. because "they" lie about everything. The diagram at this site, produced by processor manufacture ARM, (which has nothing to lose by telling it like it is), shows three wireless connectivity options per smart meter, PLUS an ability to communicate through the power system, as well as Ram, Rom, and Flash, complete with an ultra DMA hard drive controller (needed to provide storage to the flash memory) and FIVE CPU's TOTAL. ??!!??. It's a safe bet that such extreme connectivity and CPU power, plus 3 memory options could only be needed for nefarious purposes. If your refrigerator is Wifi equipped (a ridiculous RF polluting waste) when it could simply receive commands through the wiring, your refrigerator, microwave, you name it, could also be equipped with audio and visual surveillance capabilities and have that ability remain perfectly hidden, all to be transmitted out through the smart meter. With advanced devices now available for less than $10 containing microphones and video sensors, as well as buttons and flash card support, the stated $10 cost of this so called wifi device that is to be put in all appliances could easily cover the cost of the sensors as well.

But a microphone and video sensor would be obvious, and therefore they would never do it, right? Well, no. After having worked for the NSA and learning the tricks, I played around a LOT with common components no one would ever think could be used for snooping that work EXCELLENT. The most surprising of all is electronic beepers that use simple piezo drivers. The piezo element, never associated with anything other than an ability to beep makes an astonishing microphone. When properly coupled to a microphone amplifier (totally free to do at zero cost nowadays) a beeper element can be used to hear through the walls and into a detached neighboring house. That is not an exaggeration. Piezo elements are unbelievably powerful microphones, as are high impedance conventional magnetic speakers. They outperform all microphones hands down, and provide such strong input that they have to be strongly attenuated to be useful. So if your microwave or refrigerator has any ability to beep, and it is smart meter compliant, you can safely bet that it has ears that can hear you whisper from behind a closed door.

Nowadays, any device that can accept remote control commands can easily conceal a camera

My first introduction to this was with 1980's vintage Scientific Atlanta cable TV boxes (the standard back then) which all came fully equipped with CCD sensors concealed in the remote sensor, and microphones. If you can get your hands on one of them, take it apart and look. I have seen this myself. If you have ever wondered why so many open channels were available on these cable boxes, it is because the unused channels could

be accessed and used in reverse to snoop. And towards the end of their dominance these boxes still cost more than basic cable ready televisions, possibly because that CCD sensor was not cheap. What about your TV nowadays? I have not taken apart any HD televisions for a look, but knowing what happened in the past I'd say it will be a safe bet that many of these televisions will have the ability to use their remote sensor as a camera, and speakers as microphones. It's an obvious no brainer. Throw a smart meter into the mix, and there is your outgoing connection.

But WAIT, there's more!

What about the obvious ability to send signals to appliances via the home's wiring - what are the limits?

I never paid attention to this in the past, and had to take a look at the guts of one of the circuit breakers that are used in homes to do this report. These circuit breakers use an electromagnet to trip, and pass all the current that gets delivered though the breaker through that electromagnet. When the current gets high enough, the magnet pulls hard enough and trips the breaker. So I knew the frequency you could send through a breaker would be limited by this electromagnet, which will operate as a choke because it has a coil with a magnetically attractive core, which will further increase the ability of that coil to stop high frequencies from passing. Question is, how much would it really choke off the signal from a smart meter?

I no longer have my inductance meter after the Fuku report, so I cannot put it in a formula. However, I can make a guess based on experience and how things look. And my guess is that you won't get megabits to pass through it, but that it would be safe to assume you could easily get a 256 kbps connection through any household circuit breaker. Why would that be important, when wifi is megabits? Well, let me explain. Remember the dialup days, when 57.6 was the norm? How about five times that? Was it impossible to surf the web way back in the early days when the standard was 14.4? 14.4 actually worked pretty good. And even 500 baud will exceed the speed of the fastest typist. So I'd say 256kbps would represent a serious security problem if you have a power supply in your computer which can accept power line commands, switch on your hardware in secret, and raid you. I don't think this is a reality nowadays, but I do not know it is not either, and it's a safe bet with the government getting more and more snoopy that this will be a way to get into the most secure of computer systems. Forget about avoiding a CoreVPro processor, which has built in 3g, forget about removing all wifi and bluetooth - the final holy grail of information gathering would be a direct power line grab. You can bet they are working on it and your friendly smart meter will play a key role.

The following got wiped and I had to retype it, they obviously do not like the punch line . . . .

I am going to make a prediction here - that in the future, the very NEAR future, the only way you will keep a system secure is to have it run off an inverter bank, separated from the wall with a non electronic old transformer style battery charger constantly charging a battery. Filtering the smart meter signal while running directly off the line would have limited effect - If you used the right choke setup you could limit the smart meter baud rate to below 500 before you messed up the power factor too badly to run a PC, but even a 500 baud connection would only slow things down for the snoops. With patience

(and they have a lot) they could at least raid every text file off your machine, 500 baud would allow them to nail 1 kilobyte of data in approximately 18 seconds (slower than actual baud because of parity checking and other technicalities, but the answer is still clear - filtering will not be good enough. The only answer is a complete isolated disconnect from the grid.)

UPS power supplies and ordinary surge protectors will not be good enough, because surge protectors won't filter the type of signal a smart meter would produce, and a UPS could be rigged to bypass the signal from the computer directly to the line while feeding the computer inverter power. On top of this a majority of UPS power supplies do not run full time inverter anyway. Normally they keep you connected to the main and switch you over to inverter very rapidly when the power goes out, before the capacitors in your computer's power supply run out of juice. The fact that UPS power supplies normally keep you directly connected, as well as the fact that UPS power supplies usually have processors that could pass the smart meter signal along to your PC anyway makes UPS power supplies an un acceptable method of blocking snooping via the power line. The only option is an old or totally brainless 1980's style car battery charger, a battery, and a standalone inverter if data security really is that important.

I suggest governments and businesses take what I said here to heart and apply it, the ability to snoop via the power line against high priority targets is definitely possible, and definitely will be done in the future (and against the highest priority targets, is definitely happening now.) If you value your privacy, I'd implement these security measures now. Even if you have your wifi "turned off", it is not turned off. There is a separate channel that always stays open and sniffs out all available connections. And if your computer has been bugged to begin with, it will, through this back door channel, connect to any available wifi network hidden or not, and send everything you type or do straight to the NSA. And this connection will also allow "PC anywhere" type remote access to your machine. I had problems with this last night because I forgot to pull the wifi card out of the laptop I was working with, and someone went straight in and destroyed several hours of work on a machine that runs Linux and never screws up. Am I just paranoid?